REMARKS

Examiner used the wrong set of claims

Claims 25, 27, and 29 were canceled in the amendment of 06-19-2008. That amendment should have been entered as a submission in the RCE of 07-15-2008. The RCE form states "*any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise.*" Applicant did not request non-entry of any amendments. However, Examiner rejected claims 25, 27, and 29 in the present examination, indicating that he used the wrong set of claims for the examination. The claim amendments herein are based on the previous amendment of 06-19-2008. Thus it shows the current status of all claims. Applicants provide arguments herein with respect to the claims as listed herein.

Status of claims

Claims 24, 28, 30, 33-35, 37, and 40-51 are pending. Claims 24, 28, 30, 33-35, 37, and 50-51 are rejected under 35 USC 103(a) as being unpatentable over U.S. patent 7,215,775 (Noguchi et al.) in view of U.S. patent 6,947,559 (Gleeson). Claims 40-45 are rejected under 35 USC 103(a) as being unpatentable over Noguchi in view of Gleeson and U.S. patent application publication 2002/0154769 (Petersen et al). Claim 46 is rejected under 35 USC 103(a) as being unpatentable over Noguchi in view of Gleeson, and in view of Petersen, and in view of U.S. patent 6,973,499 (Peden).

Claims 24, 33, 40, 41, 44, 45, 47, and 51 are amended herein. No claims are canceled. No new claims are added. Claims 24, 28, 30, 33-35, 37, and 40-51 are presented for examination. No new matter is added.

Claim amendments herein (based on claims as amended 06-19-2008)

- Claim 24 is clarified per par. 70, lines 4-9, par. 21, and par. 22.
- Claim 33 is clarified per par. 16, and par. 59, lines 4-6.
- Various formal corrections are made for consistent terminology and antecedents.
- The indents of claims 24, 30, 40, and 47 are modified for visual clarity.
- The claim element regarding removal of high-order bits is deleted from claims 40 and 47, since it is not needed for patentability. This element is inserted in claim 41, which does not change the scope of claim 41.

No new matter is added by these amendments.

MPEP 2106 (C): "*An applicant can always amend a claim during prosecution to better reflect the intended scope of the claim.*"

Response to rejections under 35 USC 103(a)

In Applicants' claimed invention, users transmit a random number -- not an encryption key as in Noguchi (abstract). Applicants' sender and receiver then independently derive the same (symmetric) encryption key from this random number, using the same secret algorithm for key generation (pars. 9 and 10). Thus, Applicants provide benefits of asymmetric public key encryption without the disadvantages thereof (computational consumption and complex key management).

The method of Noguchi could not be used in many networking applications. This is clear from the excerpt below.

Noguchi col. 4, lines 48-52: "*The distance between both the data send/receive devices is typically less than 10 m, preferably several meters, such that a user can come and go, since the verification data needs to be compared mutually at the verification data output sections of both the data send/receive devices.*"

In other words, the sender and receiver must be in the same room, or at least in adjacent rooms. A person must walk back and forth between displays of the sender and the receiver in order to verify each transmission. Most people would avoid using this method, because they would be constantly jumping up to walk over and verify each communication. This method could not be used for transmission to a remote site, such as over the Internet, which is a main application for the present invention (par. 9).

The visual verification method taught by Noguchi cannot be automated without further complexity. He transmits an encryption key (making it potentially public) and a sample of encrypted data using that key. Thus, if he also transmitted his verification data for automatic verification, then a network snoop would have enough information to derive a decryption algorithm, because the snoop would have a sample of "before" and "after" data, and the key.

Examiner cites Noguchi FIG 13 and col. 13, lines 48-63 as indicating use of Noguchi in a public network. However, Noguchi never mentions the term "public network" or "Internet". The cited paragraph refers to an "ad-hoc" radio communication between notebook computers 88a, 88b in bags, where the notebooks are operated by respective PDAs 80a, and 80b. In this embodiment, he teaches a hybrid asymmetric/symmetric cryptosystem that increases complexity, and is not needed in Applicants' invention as claimed in the independent claims 24, 40, and 47.

Noguchi would seem to have rare application. If a sender and receiver are so close together as to use the method of Noguchi, some would prefer instead to connect using a local hardwired Ethernet with no public exposure or just a computer-to-computer data transfer cable. If a user has to walk over to the second user, some would prefer to use a flash drive to transfer files, and just walk over and confer in person rather than use email.

Combining Noguchi with other prior art to add additional features of Applicants, such as stochastic random number generation, does not change the above distinctions between Noguchi and Applicants' claimed invention. Accordingly, Noguchi cannot support 35 USC 103 rejections of the present claims, because it cannot produce the invention as claimed.

Present claims 24, 40, 47, and 50-51 recite a stochastic random number obtained from operational measurements in an automation system. This is significant because numerous operational measurements are already available in an automation system without additional hardware. This eliminates the need for a dedicated stochastic random number generator as required in Gleeson. He teaches special hardware to provide stochastic processes using technology of early liquid crystal displays (par. 3, lines 57-62). This clearly requires additional hardware not currently used in automation systems. For at least this reason, combining Gleeson with Noguchi would not produce the invention as claimed, and does not support the present rejection for claims 24, 40, 47, and 50-51. Applicants' operational measurement source allows combinations of stochastic operational measurements to be used for symmetric key generation, as described in par. 65, and as claimed in claims 50-51. This provides maximum unpredictability without additional hardware.

The method of Noguchi would be impractical to modify according to the present dependent claims 33-35, because each automatic or master-controlled request to generate an encryption key would require at least one user to jump up and walk to the other user, thus interrupting their work.

Regarding claim 41: Examiner has asserted that it would be an obvious design choice to use the least significant bits of measured data to generate an encryption key. In par. 31 of the present Office Action, he refers to Petersen par. 39. However par. 39 of Petersen teaches avoiding deletion of high order bits of data, and thus explicitly teaches away from Applicants' method, supporting Applicants' argument below. Deletion of high order bits is an overflow, which is a "fatal" or terminal error, and is displayed as such on all calculators.

> Petersen par. 39, lines 6-12 : "*The position of the decimal separator in a fixed-point number is a weighting between digits in the integer part and digits in the fraction part of the number. To achieve the best result of a calculation, it is usually desired to include as many digits after the decimal separator as possible, to obtain the highest resolution. However, it may also be important to assign enough bits to the integer part to ensure that no overflow will occur. Overflow is loading or calculating a value into a register that is unable to hold a number as big as the*

> *value loaded or calculated. Overflow results in deletion of the most significant bits (digits) and possible sign change.*"

A design choice is one of several known options that are similarly good choices. However, removing high-order bits from measurement data normally destroys the data. For example, assume a time series of 8-bit measurement data has a range from binary 00100101 to 01110011 (decimal 37 to 115). If you remove the top 2 bits, the data is limited to a maximum value of 111111, or decimal 63. This causes an overflow for any values greater than 63, eliminating the most significant portion of such values and destroying the data. Therefore this would certainly not be done without some non-obvious reason. If the high-order bit represents the sign (+ or -), then eliminating it also destroys the data because one cannot determine if a measured value was positive or negative. The goal of a random number is unpredictability. The more significant bits there are in a random number, the less predictable and harder to guess it is, thus the more secure it is as a seed value for an encryption key. The above factors teach away from using only the least significant bits, either for data or for security key generation. For these reasons, the method of claim 41 is not supported by general knowledge, and is not an obvious design choice.

> MPEP 2142 Legal Concept of *Prima Facie* Obviousness [R-6]: "*The tendency to resort to "hindsight" based upon applicant's disclosure is often difficult to avoid due to the very nature of the examination process. However, impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art.*"

Conclusion

M.P.E.P. 2143.03 provides that to establish prima facie obviousness of a claimed invention, all words in a claim must be considered in judging the patentability of that claim against the prior art. If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious.

For obviousness under 35 USC 103, a combination must be suggested by the references or motivated by expected benefits in view of documented knowledge in the field at the time of the invention, not by hindsight guided by Applicant's invention. The combination should not be contrary to the teachings of the references, it must work, and it must produce the Applicant's invention. These criteria are not met by the cited combinations as argued above. Thus, Applicants feel this application is in condition for allowance, which is respectfully requested.

The commissioner is hereby authorized to charge any appropriate fees due in connection with this paper, including fees for additional claims and terminal disclaimer fee, or credit any overpayments to Deposit Account No. 19-2179.

Respectfully submitted,

Dated: 10/29/08

By: _____

John P. Musone
Registration No. 44,961
(407) 736-6449

Siemens Corporation
Intellectual Property Department
170 Wood Avenue South
Iselin, New Jersey 08830